



FR 01/1205

# BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

4

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 17 MAI 2001

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

A handwritten signature in black ink, appearing to read 'M. Planche', enclosed within a large, loopy oval stroke.

Martine PLANCHE

### DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS  
CONFORMÉMENT À LA  
RÈGLE 17.1.a) OU b)

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint Petersburg  
75800 PARIS cedex 08  
Téléphone : 01 53 04 53 04  
Télécopie : 01 42 93 59 30  
<http://www.inpi.fr>

**THIS PAGE BLANK (USPTO)**

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W / 260899

<p>REMISE DES PIÈCES</p> <p>DATE <b>24 NOV 2000</b></p> <p>LIEU <b>75 INPI PARIS</b></p> <p>N° D'ENREGISTREMENT <b>0015215</b></p> <p>NATIONAL ATTRIBUÉ PAR L'INPI</p> <p>DATE DE DÉPÔT ATTRIBUÉE <b>24 NOV. 2000</b></p> <p>PAR L'INPI</p>		<p><b>1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE</b></p> <p><b>Frédéric BENECH</b> <i>Avocat à la Cour</i> <b>69, avenue Victor Hugo</b> <b>75783 PARIS CEDEX 16 - (FRANCE)</b></p>	
<p><b>Vos références pour ce dossier</b> (facultatif) <b>B0266A</b></p>			
<p><b>Confirmation d'un dépôt par télécopie</b> <input type="checkbox"/> N° attribué par l'INPI à la télécopie</p>			
<p><b>2 NATURE DE LA DEMANDE</b></p> <p>Demande de brevet <input checked="" type="checkbox"/></p> <p>Demande de certificat d'utilité <input type="checkbox"/></p> <p>Demande divisionnaire <input type="checkbox"/></p> <p><i>Demande de brevet initiale</i> N° _____ Date : / /</p> <p><i>ou demande de certificat d'utilité initiale</i> N° _____ Date : / /</p> <p>Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i> <input type="checkbox"/> N° _____ Date : / /</p>		<p><b>Cochez l'une des 4 cases suivantes</b></p>	
<p><b>3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)</b></p> <p><b>PROCEDE ET DISPOSITIF DE CERTIFICATION</b></p>			
<p><b>4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE</b></p>		<p>Pays ou organisation <b>FRANCE</b> N° <b>00 13101</b></p> <p>Date <b>04/10/2000</b></p> <p>Pays ou organisation _____ N° _____</p> <p>Date / /</p> <p>Pays ou organisation _____ N° _____</p> <p>Date / /</p> <p><input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»</p>	
<p><b>5 DEMANDEUR</b></p> <p>Nom ou dénomination sociale <b>MAGICAXESS</b></p> <p>Prénoms _____</p> <p>Forme juridique <b>société anonyme</b></p> <p>N° SIREN _____</p> <p>Code APE-NAF _____</p> <p>Adresse</p> <p>Rue <b>28, rue Jean-Jaurès</b></p> <p>Code postal et ville <b>92800 PUTEAUX</b></p> <p>Pays <b>FRANCE</b></p> <p>Nationalité <b>Française</b></p> <p>N° de téléphone (facultatif) _____</p> <p>N° de télécopie (facultatif) _____</p> <p>Adresse électronique (facultatif) _____</p>		<p><input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»</p>	

Réservé à l'INPI

REMISE DES PIÈCES

DATE

24 NOV 2000

LIEU

75 INPI PARIS

N° D'ENREGISTREMENT

NATIONAL ATTRIBUÉ PAR L'INPI

0015215

DB 540 W / 260899

**Vos références pour ce dossier :**

(facultatif)

B0266A

**6 MANDATAIRE**

Nom

BENECH

Prénom

Frédéric

Cabinet ou Société

N° de pouvoir permanent et/ou  
de lien contractuel

9148

Adresse

Rue

69, avenue Victor-Hugo

Code postal et ville

75783 PARIS CEDEX 16

N° de téléphone (facultatif)

01 44 17 36 60

N° de télécopie (facultatif)

01 40 67 91 40

Adresse électronique (facultatif)

benech@benech.com

**7 INVENTEUR (S)**

Les inventeurs sont les demandeurs

☐ Oui

☒ Non Dans ce cas fournir une désignation d'inventeur(s) séparée

**8 RAPPORT DE RECHERCHE**

Uniquement pour une demande de brevet (y compris division et transformation)

Établissement immédiat  
ou établissement différé

☒

☐

Paiement échelonné de la redevance

Paiement en trois versements, uniquement pour les personnes physiques

☐ Oui

☐ Non

**9 RÉDUCTION DU TAUX  
DES REDEVANCES**

Uniquement pour les personnes physiques

☐ Requête pour la première fois pour cette invention (joindre un avis de non-imposition)

☐ Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence):

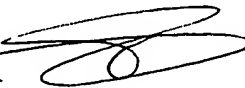
Si vous avez utilisé l'imprimé «Suite»,  
indiquez le nombre de pages jointes

**10 SIGNATURE DU DEMANDEUR  
OU DU MANDATAIRE  
(Nom et qualité du signataire)**



Frédéric BENECH Avocat à la Cour

**VISA DE LA PRÉFECTURE  
OU DE L'INPI**



DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg

75800 Paris Cedex 08


Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1. / .1.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

<b>Vos références pour ce dossier</b> (facultatif)		B0266A	
<b>N° D'ENREGISTREMENT NATIONAL</b>		00 15215	
<b>TITRE DE L'INVENTION</b> (200 caractères ou espaces maximum)  PROCÉDE ET DISPOSITIF DE CERTIFICATION			
<b>LE(S) DEMANDEUR(S) :</b>  BENECH Frédéric avocat à la Cour 69, avenue Victor-Hugo F-75783 PARIS CEDEX 16			
<b>DESIGNE(NT) EN TANT QU'INVENTEUR(S) :</b> (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		KREMER	
Prénoms		Gilles	
Adresse	Rue	34, avenue de la Paix	
	Code postal et ville	92170	VANVES
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
<b>DATE ET SIGNATURE(S)</b> <b>DU (DES) DEMANDEUR(S)</b> <b>OU DU MANDATAIRE</b> (Nom et qualité du signataire)		Le 27 décembre 2000  Frédéric BENECH Avocat à la Cour  	

5

## PROCEDE ET DISPOSITIF DE CERTIFICATION

10

La présente invention concerne un procédé et un dispositif de certification. En particulier, la présente invention concerne la transmission de données en ligne, par exemple sur le réseau Internet.

15

Du fait de sa nature ouverte, Internet a augmenté les besoins de sécurité de transmission de données. En effet, l'architecture même de l'Internet le rend particulièrement vulnérable : le protocole IP, totalement décentralisé, fait circuler les "datagrammes," ou paquets sans qu'ils soient protégés. Les adresses IP elles-mêmes, gérées par les DNS (Domain Name Servers pour serveurs de noms de domaines), ne sont pas à l'abri d'actions de malveillance. Les systèmes d'exploitation ont des failles de sécurité. D'où une liste impressionnante de menaces :

20

- écoute de paquets ou "sniffing";
- substitution de paquets ou "spoofing";
- piratage de DNS;
- déni de service;
- intrusions; et
- dissémination de programmes malveillants, virus et chevaux de Troie.

25

30

La cryptologie n'a pas réponse à toutes ces questions. En cryptologie, une clé est insérée au moment du chiffrement des données afin d'assurer la confidentialité de celles-ci. Les différentes normes de sécurité disponibles, pour le courrier électronique, pour les sessions de communication du web (SSL ou Secure Socket Layer pour couche de sécurité), pour le protocole IP lui-même (IPsec), mettent en oeuvre tout l'arsenal des méthodes modernes : authentification et signature, échange de clé conventionnelle, chiffrement symétrique. Des centaines de millions de clés RSA ont ainsi été produites.

Il se pose alors de nouveaux problèmes : comment gérer ces clés ? Comme le note Jacques Stern, Directeur du Département Informatique de l'Ecole Normale

Supérieure "il est illusoire d'utiliser un chiffrement RSA en laissant traîner ses clés secrètes sur un disque dur mal protégé contre les intrusions" (Dans un article publié dans Le Monde daté du 12 septembre 2000). En outre se pose la question de lier une clé publique RSA à son propriétaire légitime.

5 La présente invention entend remédier à tout ou partie de ces inconvénients. A cet effet, la présente invention vise, selon un premier aspect, un procédé de certification, caractérisé en ce qu'il comporte :

- 10 - une opération de transmission de données depuis un système informatique émetteur à un système informatique récepteur, sur un premier support de communication,
- une opération de génération d'une trace desdites données représentatives desdites données, par le système informatique récepteur,
- une opération de transmission d'une partie de ladite trace à un dispositif de communication, sur un deuxième support de communication différent du
- 15 premier support de communication,
- une opération de réception de ladite partie de trace par le système informatique émetteur,
- une opération de transmission de ladite partie trace depuis le système informatique émetteur au système informatique récepteur, et
- 20 - une opération de vérification de la correspondance de la partie de trace reçue par le système informatique récepteur avec la trace générée par le système informatique récepteur.

Grâce à ces dispositions, la partie de trace est liée auxdites données et peut servir à détecter une modification ultérieure desdites données.

25 Selon des caractéristiques particulières du procédé tel que succinctement exposé ci-dessus, ladite trace est représentative d'un condensatdesdites données.

Grâce à ces dispositions, la partie de trace permet de détecter toute modification ultérieure desdites données.

30 Selon des caractéristiques particulières, le procédé tel que succinctement exposé ci-dessus comporte une opération de transmission d'un identifiant d'un utilisateur du système informatique émetteur.

Grâce à ces dispositions, une authentification de l'utilisateur du système informatique émetteur ou une signature électronique peuvent être effectuées.

Selon des caractéristiques particulières, le procédé tel que succinctement exposé ci-dessus comporte une opération de mise en correspondance dudit identifiant avec une adresse du dispositif de communication sur le deuxième support de communication.

5 Grâce à ces dispositions, l'adresse du dispositif de communication est une adresse qui correspond à l'utilisateur du système informatique émetteur.

Selon des caractéristiques particulières du procédé tel que succinctement exposé ci-dessus, ladite trace est représentative d'une clé privée conservée par le système informatique récepteur.

10 Grâce à ces dispositions, le système informatique récepteur effectue une signature desdites données.

Selon des caractéristiques particulières, le procédé tel que succinctement exposé ci-dessus, comporte une opération de mise en correspondance dudit identifiant avec ladite clé privée.

15 Grâce à ces dispositions, le système informatique récepteur effectue une signature desdites données au nom de l'utilisateur du système informatique émetteur.

Selon des caractéristiques particulières, le procédé tel que succinctement exposé ci-dessus, comporte une opération de troncature de ladite trace, et en ce que au cours de l'opération de transmission d'au moins une partie de ladite trace, le résultat de  
20 ladite troncature est transmis.

Grâce à ces dispositions, la partie de ladite trace comporte moins de symboles que ladite trace.

Selon des caractéristiques particulières du procédé tel que succinctement exposé ci-dessus, le premier support de communication est l'Internet.

25 Grâce à ces dispositions, les données peuvent être transmises depuis n'importe quel système informatique relié à l'Internet.

Selon des caractéristiques particulières du procédé tel que succinctement exposé ci-dessus, le deuxième support de communication est un réseau sans fil.

30 Grâce à ces dispositions, l'authentification de l'utilisateur du système informatique émetteur peut être effectuée en tout lieu.

Selon des caractéristiques particulières du procédé tel que succinctement exposé ci-dessus, au cours de l'opération de transmission desdites données, un identifiant d'un système informatique destinataire est transmis, ledit procédé comportant une



opération de transmission desdites données depuis le système informatique récepteur à un système informatique destinataire.

Grâce à ces dispositions, le système informatique récepteur peut servir d'intermédiaire dans une transmission entre le système informatique émetteur et le système informatique destinataire. Il peut, en outre, assurer des fonctions de datage, de  
5 notarisation ou de certification de remise en main propre au destinataire desdites données.

Selon des caractéristiques particulières, le procédé tel que succinctement exposé ci-dessus comporte une opération de mise en correspondance desdites données avec une clé publique et en ce que au cours de l'opération de transmission desdites  
10 données audit système informatique destinataire, ladite clé publique est transmise.

Grâce à ces dispositions, Le destinataire desdites données peut vérifier l'identité de l'émetteur desdites données, par la mise en oeuvre de la clé publique.

Selon des caractéristiques particulières, le procédé tel que succinctement exposé ci-dessus comporte une opération de génération d'une information confidentielle  
15 par le système informatique récepteur et une opération de transmission à un deuxième dispositif de communication d'une information confidentielle à une dispositif de communication sur le deuxième support de communication, par le système informatique récepteur, une opération de réception de ladite information confidentielle par le système informatique récepteur, sur le premier moyen de communication et une opération de  
20 vérification de correspondance entre l'information confidentielle transmise par le système informatique récepteur avec l'information confidentielle reçue par le système informatique récepteur.

Grâce à ces dispositions, le destinataire desdites données est authentifié.

La présente invention vise aussi un dispositif de certification, caractérisé  
25 en ce qu'il comporte :

- un moyen de transmission de données depuis un système informatique émetteur à un système informatique récepteur, sur un premier support de communication,
- un moyen de génération d'un trace desdites données représentatives desdites  
30 données, par le système informatique récepteur,
- un moyen de transmission d'au moins une partie de ladite trace à un dispositif de communication, sur un deuxième support de communication différent du premier support de communication,
- un moyen de réception de ladite trace par le système informatique émetteur,

- un moyen de transmission de ladite trace depuis le système informatique émetteur au système informatique récepteur, et
- un moyen de vérification de la correspondance de la trace reçue par le système informatique récepteur et de la trace générée par le système informatique récepteur.

Les caractéristiques particulières et les avantages dudit dispositif correspondent aux caractéristiques particulières et avantages du procédé tels que succinctement exposé ci-dessus.

- D'autres avantages, buts et caractéristiques de la présente invention ressortiront de la description qui va suivre faite en regard du dessin annexé dans lequel :
- la figure 1 représente une succession d'opérations effectuées par un terminal utilisateur et un serveur de certification, dans un mode de réalisation particulier de la présente invention ;
  - la figure 2 représente une succession d'opérations effectuées par un terminal utilisateur et le serveur de certification, dans un autre mode de réalisation particulier de la présente invention ;
  - la figure 3 représente une succession d'opérations effectuées par un terminal utilisateur et le serveur de certification, dans un autre mode de réalisation particulier de la présente invention ; et
  - la figure 4 représente un organigramme de mise en oeuvre d'un autre mode de réalisation de la présente invention.

En figure 1 sont représentés un poste utilisateur ou système informatique émetteur 100, une application Internet 110, une salle blanche 120, une mémoire de stockage 130, un deuxième réseau de communication 140 et un récepteur 150 sur le deuxième réseau de communication 140. La salle blanche 120 comporte une protection pare-feu (en anglais "firewall") 160, un serveur de sécurité 170 et un générateur de certificats 180. Les opérations effectuées dans le mode de réalisation particulier illustré en figure 1 sont représentées dans des rectangles et numérotées de 1 à 12. L'application Internet 110 et la salle blanche 120 sont conjointement appelé système informatique récepteur.

Le poste utilisateur 100 est, par exemple, un ordinateur personnel (PC), un ordinateur de réseau (NC) ou un assistant numérique personnel (en anglais Personal Digital Assistant ou PDA). Le poste utilisateur 100 est doté d'un logiciel de communication à distance pour mettre en oeuvre l'application Internet 110, conjointement

avec le serveur de sécurité 170. Ce logiciel de communication à distance peut être un logiciel de navigation ou un logiciel de courrier électronique, par exemple.

L'application Internet 110 permet la communication entre le poste utilisateur 100 et le serveur de sécurité 170 et la transmission de données depuis le poste utilisateur 100 vers la mémoire de stockage 130, par exemple par l'intermédiaire du serveur de sécurité 170. La salle blanche 120 est un espace protégé contre toute intrusion physique, telle qu'une salle de coffre d'une banque. La mémoire de stockage 130 est une mémoire adaptée à conserver des données pendant une longue période, qui dépasse une année.

Le deuxième réseau de communication 140 est, par exemple, un réseau téléphonique et, encore plus particulièrement un réseau de téléphonie mobile ou de récepteurs alphanumériques communément appelés "pageurs". Le deuxième réseau 140 est appelé "deuxième" par comparaison avec le réseau Internet, que l'on nomme aussi "premier" réseau dans la suite de la présente demande de brevet. Le deuxième réseau 140 est adapté à transmettre une clé ou certificat depuis le serveur de sécurité 170 jusqu'au récepteur 150. Le récepteur 150 sur le deuxième réseau 140 peut, selon le type de deuxième réseau 140, être un téléphone mobile, un pageur ou un récepteur quelconque. Le récepteur 150 permet à l'utilisateur du poste utilisateur 100 de prendre connaissance d'informations transmises par le serveur de sécurité 170.

La protection pare-feu 160 est de type matérielle et/ou logicielle et interdit toute intrusion logicielle dans le serveur de sécurité 170. Le serveur de sécurité 170 est un serveur informatique de type connu. Enfin, le générateur de certificats 180 est adapté à générer des certificats jetables, par exemple de type conforme à la norme X509-V3.

Le poste utilisateur 100 et le serveur de sécurité 170 sont conjointement adaptés à mettre en oeuvre les opérations indiquées ci-dessous. Par exemple, le serveur de sécurité 170 est adapté à fournir des routines applicatives ou "applets" au poste utilisateur 100.

Au début du processus de certification, on suppose que des données sont à transmettre de manière certifiée et signée depuis le poste utilisateur 100 jusqu'à la mémoire de stockage 130. L'utilisateur du poste utilisateur 100 se connecte au serveur de sécurité 120 pour lancer le processus de certification.

Au cours de l'opération 1, après identification de l'utilisateur su poste utilisateur 100, l'application Internet 110 télécharge une routine applicative certifiée et signée dans le poste utilisateur 100. On observe que la routine applicative en question

peut n'être téléchargée que dans le cas où une copie de cette routine n'est pas déjà implantée dans le poste utilisateur 100. Cette caractéristique particulière permet de rendre portable le procédé de certification objet de la présente invention, sans ralentir ce processus dans le cas où l'utilisateur met successivement en oeuvre le même poste

5 utilisateur 100, pour plusieurs certifications de données. Au cours de l'opération 2, le générateur de certificats 180 génère un certificat jetable, par exemple sous la forme d'une clé privée conforme à la norme X509-V3. Par exemple, le certificat jetable est généré aléatoirement par le générateur 180.

10 Au cours de l'opération 3, le serveur de sécurité 170 transmet le certificat jetable au poste utilisateur 100. Au cours de l'opération 4, le poste utilisateur 100 met en oeuvre la routine applicative téléchargée au cours de l'opération 1 pour obtenir une trace des données à transmettre, appelé condensâ (en anglais "hash"), trace qui dépend du certificat jetable généré au cours de l'opération 2 et des données à transmettre et qui permet la détection de toute modification ultérieure des données à transmettre.

15 Au cours de l'opération 5, les données à transmettre et le condensâ sont téléchargés depuis le poste utilisateur 100 jusqu'à l'application Internet 110. De plus, des coordonnées de chaque destinataire des données à transmettre est transmis par le poste utilisateur 100 à l'application Internet 110. Ces coordonnées peuvent prendre la forme d'adresse de courrier électronique (en anglais "e-mail"), de numéro de téléphone ou de

20 tout autre type d'information permettant de contacter chaque destinataire des données à transmettre. Au cours de l'opération 6, l'intégrité des données à transmettre est vérifiée, en mettant en oeuvre la clé jetable générée au cours de l'opération 2 et le condensâ.

On observe qu'à la fin de l'opération 6, une copie des données à transmettre à été faite depuis le poste utilisateur 100 dans l'application Internet 110 et que cette copie

25 est certifiée conforme à l'original grâce à la mise en oeuvre d'une clé jetable. Pour éviter que le certificat jetable soit réutilisé, au cours de l'opération 10, le certificat jetable est révoqué, c'est-à-dire qu'il devient inutilisable pour certifier des données.

En variante, le certificat jetable généré au cours de l'opération 2 est un certificat à durée de vie très courte, préférentiellement inférieure à une heure. Dans cette

30 variante, l'opération 10 n'est pas exécutée puisqu'au delà de la durée de vie du certificat jetable, ce certificat n'est pas utilisable pour certifier des données.

Les opérations 7 et 8 correspondent à un exemple de signature pouvant être utilisé en combinaison avec les opérations 1 à 6 ci-dessus. Au cours de l'opération 7, un sceau secret est généré et transmis, par l'intermédiaire du deuxième réseau 140, au

récepteur 150. L'adresse du récepteur 150 sur le deuxième réseau est déterminée en mettant en correspondance l'identifiant de l'utilisateur transmis au cours de l'opération 1 avec ladite adresse, dans une table de correspondance. Préférentiellement, le sceau secret est calculé sur les éléments de signature du document. Préférentiellement, le sceau secret  
5 dépend des données à transmettre, de leur nombre, de leur contenu, de la date et de l'heure de la génération du sceau secret, de la clé privée de l'émetteur des données déterminée en correspondance avec l'identifiant de l'utilisateur transmis au cours de l'opération 1, de l'adresse internet ("adresse IP") du poste utilisateur 100 et/ou d'un numéro de la session Internet au cours de laquelle les données sont transmises. Selon un exemple de mise en  
10 oeuvre de l'opération 7, le sceau secret est obtenu par calcul d'un condensâ des données à transmettre, par exemple sous la forme d'une séquence de vingt symboles, de chiffrement de ce condensâ par la clé privée de l'utilisateur du poste utilisateur 100, et d'extraction d'une partie du résultat de ce chiffrement, par exemple huit symboles sur vingt.

Le lecteur pourra se référer à la figure 4 et/ou à la demande de brevet  
15 PCT/FR98/02348 pour mieux connaître des exemples d'étapes mises en oeuvre au cours des opérations 7 et 8. Au cours de l'opération 8, l'utilisateur commun du poste utilisateur 100 et du récepteur 150 saisie le sceau secret et ce sceau secret est transmis au serveur de sécurité 170 où le sceau est vérifié, opération 9.

En variante, les opérations 7 à 9 sont remplacées par une opération de  
20 signature basée sur l'utilisation d'une carte à mémoire ("carte à puce") ou d'une mesure de biométrie.

A la fin de l'opération 8, les données transmises sont donc certifiées intègres et signées par l'utilisateur qui les transmet. L'opération 9 consiste à substituer une signature dite PKI (pour Public Key Infrastructure, soit infrastructure de clés publiques) à  
25 la signature effectuée au cours des opérations 7 et 8.

Au cours de l'opération 9, les données transmises sont signées avec la clé privée de l'utilisateur qui les a transmise (dit "signataire" des données).

Enfin, au cours de l'opération 11, les données transmises, certifiées et signées par clé privée sont transmises à la mémoire de stockage 130 avec une date de telle  
30 manière qu'elles sont horodatées, archivées et notarisée.

Dans une application de la présente invention à une remise en main propre des données transmises, un destinataire est, à la suite de l'opération 11, averti de la mise à sa disposition des données à transmettre et des opérations similaires aux opérations exposées ci-dessus sont mises en oeuvre pour effectuer une copie certifiée conforme sur

le poste utilisateur du destinataire après avoir recueilli de sa part une signature. Par exemple, une signature telle qu'exposée dans la demande de brevet PCT/FR98/02348 peut, de nouveau être mise en oeuvre pour authentifier le destinataire. Un exemple d'une succession d'opérations mises en oeuvre pour cette remise en main propre est donné en

5 figure 2.

En figure 2 sont représentés un poste utilisateur destinataire ou système informatique destinataire 200, l'application Internet 110, la salle blanche 120, la mémoire de stockage 130, le deuxième réseau de communication 140 et un récepteur 250 sur le deuxième réseau de communication 140. Les opérations effectuées dans le mode de

10 réalisation particulier illustré en figure 2 sont représentées dans des rectangles et numérotées de 13 à 25. Ces opérations peuvent suivre les opérations 1 à 12 illustrées en figure 1 et effectuées en relation avec un poste utilisateur 100 généralement différent du poste utilisateur 200.

Le poste utilisateur destinataire 200 est, par exemple, un ordinateur

15 personnel (PC), un ordinateur de réseau (NC) ou un assistant numérique personnel (en anglais Personal Digital Assistant ou PDA). Le poste utilisateur destinataire 200 est doté d'un logiciel de communication à distance pour mettre en oeuvre l'application Internet 110, conjointement avec le serveur de sécurité 170. Ce logiciel de communication à distance peut être un logiciel de navigation ou un logiciel de courrier électronique, par

20 exemple.

L'application Internet 110 permet la communication entre le poste utilisateur 200 et le serveur de sécurité 170 et la transmission de données depuis le poste utilisateur 200 vers la mémoire de stockage 130, par exemple par l'intermédiaire du serveur de sécurité 170.

25 Le récepteur 250 sur le deuxième réseau 140 peut, selon le type de deuxième réseau 140, être un téléphone mobile, un pageur ou un récepteur quelconque. Le récepteur 250 permet à l'utilisateur du poste utilisateur destinataire 200 de prendre connaissance d'informations transmises par le serveur de sécurité 170.

Le poste utilisateur destinataire 200 et le serveur de sécurité 170 sont

30 conjointement adaptés à mettre en oeuvre les opérations indiquées ci-dessous. Par exemple, le serveur de sécurité 170 est adapté à fournir des routines applicatives ou "applets" au poste utilisateur destinataire 200.

Au début du processus de certification, on suppose que des données sont à transmettre de manière certifiée et signée depuis la mémoire de stockage 130 jusqu'au poste utilisateur destinataire 200.

5 L'utilisateur du poste utilisateur destinataire 200 se connecte initialement au premier réseau, par exemple pour consulter des courriers électroniques.

Au cours de l'opération 13, l'application Internet 110 émet à destination du poste utilisateur destinataire 200 un courrier électronique (e-mail) qui indique que de l'information est mise à disposition de l'utilisateur du poste 200.

10 Au cours de l'opération 14, l'utilisateur accède à l'application interne 110 en sélectionnant son adresse Internet. Au cours de l'opération 15, l'application Internet 110 télécharge une routine applicative certifiée dans le poste utilisateur destinataire 200. On observe que la routine applicative en question peut n'être téléchargée que dans le cas où une copie de cette routine n'est pas déjà implantée dans le poste utilisateur 200. Cette caractéristique particulière permet de rendre portable le procédé de certification objet de  
15 la présente invention, sans ralentir ce processus dans le cas où l'utilisateur met successivement en oeuvre le même poste utilisateur destinataire 200, pour recevoir plusieurs ensembles données. On observe que les routines applicatives téléchargées au cours des opérations 1 et 15 peuvent être identiques pour permettre d'une part la transmission de données vers la mémoire 130 et, d'autre part, pour recevoir des données  
20 depuis cette mémoire.

Les opérations 16 et 17 correspondent à un exemple de signature pouvant être utilisé en combinaison avec les opérations 13 à 15 ci-dessus. Au cours de l'opération 16, un sceau secret est généré et transmis, par l'intermédiaire du deuxième réseau 140, au récepteur 250. Préférentiellement, le sceau secret est calculé sur les éléments de signature  
25 du document. Préférentiellement, le sceau secret dépend des données à transmettre, de leur nombre, de leur contenu, de la date et de l'heure de la génération du sceau, et/ou d'un numéro de la session Internet au cours de laquelle les données sont transmises. Le lecteur pourra se référer à la demande de brevet PCT/FR98/02348 pour mieux connaître des exemples d'étapes mises en oeuvre au cours des opérations 16 et 17. Au cours de  
30 l'opération 17, l'utilisateur commun du poste utilisateur destinataire 200 et du récepteur 250 saisie le sceau secret sur le poste utilisateur destinataire 200 et ce sceau secret est transmis au serveur de sécurité 170 où le sceau est vérifié. A la fin de l'opération 17, les données transmises sont donc certifiées intègres et signées par l'utilisateur qui les transmet.

En variante, les opérations 16 et 17 sont remplacées par une opération de signature basée sur l'utilisation d'une carte à mémoire ("carte à puce") ou d'une mesure de biométrie.

Au cours de l'opération 18, le générateur de certificats 180 génère un  
 5 certificat de retrait, par exemple sous la forme d'une clé conforme à la norme X509-V3. Le certificat de retrait contient la clé publique de l'utilisateur du poste utilisateur 100. Au cours de l'opération 19, le serveur de sécurité 170 transmet le certificat de retrait au poste utilisateur destinataire 200. Au cours de l'opération 20, l'application 110 détermine un condensâ des données à transmettre, qui dépend du certificat de retrait généré au cours de  
 10 l'opération 18 et des données à transmettre et qui permet la détection de toute modification ultérieure des données à transmettre.

Au cours de l'opération 21, les données à transmettre et le condensâ sont téléchargés depuis l'application Internet 110 jusqu'au poste utilisateur destinataire 200. Au cours de l'opération 22, l'intégrité des données à transmettre est vérifiée, en mettant en  
 15 oeuvre la clé publique contenue dans le certificat de retrait généré au cours de l'opération 18 et le condensâ.

On observe qu'à la fin de l'opération 22, une copie des données à transmettre à été faite depuis la mémoire de stockage 130 jusqu'au poste utilisateur destinataire 200 et que cette copie est certifiée conforme à l'original grâce à la mise en  
 20 oeuvre d'une clé jetable. Au cours de l'opération 23, un accusé de réception d'intégrité est transmis depuis le terminal utilisateur destinataire 200 vers le serveur de sécurité 170. Cet accusé de réception d'intégrité témoigne que les données à transmettre ont été transmises au terminal utilisateur destinataire 200 de manière intègre, c'est à dire que les données à transmettre n'ont pas été modifiées après l'opération 20.

Au cours de l'opération 24, une trace de la transmission des données à l'utilisateur destinataire est certifiée et mémorisée dans la mémoire de stockage 130. Cette  
 25 date est associée aux données transmises et est ainsi horodatées, archivées et notarisée. Au cours de l'opération 25, le serveur de sécurité met à disposition de l'émetteur des données transmises un accusé de réception qui l'informe que les données qu'il à transmise  
 30 au cours de l'opération 4 ont été reçues par l'un de leur destinataire. On observe qu'un accusé de réception est transmis à l'émetteur des données pour chacun des destinataires des données.

En figure 3 sont représentés le poste utilisateur ou système informatique émetteur 100, une application Internet 310, la salle blanche 120, la mémoire de stockage



130, le deuxième réseau de communication 140 et le récepteur 150 sur le deuxième réseau de communication 140. Les opérations effectuées dans le mode de réalisation particulier illustré en figure 3 sont représentées dans des rectangles et numérotées de 31 à 42. L'application Internet 310 et la salle blanche sont conjointement appelées système informatique récepteur.

Le poste utilisateur 100 et le serveur de sécurité 170 sont conjointement adaptés à mettre en oeuvre les opérations 31 à 42 indiquées ci-dessous. Au début du processus de certification, on suppose que plusieurs ensembles de données sont à transmettre de manière certifiée et signée depuis le poste utilisateur 100 jusqu'à la mémoire de stockage 130. L'utilisateur du poste utilisateur 100 se connecte au serveur de sécurité 120 pour lancer le processus de certification.

Au cours de l'opération 31, après identification de l'utilisateur du poste utilisateur 100, l'application Internet 310 télécharge une routine applicative certifiée dans le poste utilisateur 100. On observe que la routine applicative en question peut n'être téléchargée que dans le cas où une copie de cette routine n'est pas déjà implantée dans le poste utilisateur 100. Cette caractéristique particulière permet de rendre portable le procédé de certification objet de la présente invention, sans ralentir ce processus dans le cas où l'utilisateur met successivement en oeuvre le même poste utilisateur 100, pour plusieurs certifications de données. Au cours de l'opération 32, le générateur de certificats 180 génère un certificat jetable, par exemple sous la forme d'une clé privée conforme à la norme X509-V3. Par exemple, le certificat jetable est généré aléatoirement par le générateur 180.

Au cours de l'opération 33, le serveur de sécurité 170 transmet le certificat jetable au poste utilisateur 100. Au cours de l'opération 34, l'utilisateur sélectionne explicitement chacun des ensembles de données à transmettre. Par exemple, l'utilisateur du poste utilisateur 100 sélectionne, un par un, des fichiers à transmettre, chaque fichier constituant un ensemble de données à transmettre.

Toujours au cours de l'opération 34, le poste utilisateur 100, met en oeuvre la routine applicative téléchargée au cours de l'opération 31 pour obtenir un condensé de chacun des ensembles de données à transmettre, qui dépend du certificat jetable généré au cours de l'opération 32 et des données dudit ensemble. Chaque condensé permet la détection de toute modification ultérieure d'un ensemble de données à transmettre.

Au cours de l'opération 35, les ensembles données à transmettre et les condensés sont téléchargés depuis le poste utilisateur 100 jusqu'à l'application Internet

310. De plus, des coordonnées de chaque destinataire de chaque ensemble de données à transmettre est transmis par le poste utilisateur 100 à l'application Internet 110. Ces coordonnées peuvent prendre la forme d'adresse de courrier électronique (en anglais "e-mail"), de numéro de téléphone ou de tout autre type d'information permettant de  
 5 contacter chaque destinataire des données à transmettre. Au cours de l'opération 36, l'intégrité des ensembles de données à transmettre est vérifiée, en mettant en oeuvre la clé jetable générée au cours de l'opération 32 et les condensâ.

On observe qu'à la fin de l'opération 36, une copie des ensembles de données à transmettre a été faite depuis le poste utilisateur 100 dans l'application Internet  
 10 310 et que cette copie des ensembles de données est certifiée conforme à l'original grâce à la mise en oeuvre d'une clé jetable. Pour éviter que le certificat jetable soit réutilisé, au cours de l'opération 40, le certificat jetable est révoqué, c'est-à-dire qu'il devient inutilisable pour certifier des ensembles de données.

En variante, le certificat jetable généré au cours de l'opération 32 est un  
 15 certificat à durée de vie très courte, préférentiellement inférieure à une heure. Dans cette variante, l'opération 10 n'est pas exécutée puisqu'au delà de la durée de vie du certificat jetable, ce certificat n'est pas utilisable pour certifier des données.

Les opérations 37 et 38 correspondent à un exemple de signature pouvant être utilisé en combinaison avec les opérations 31 à 36 ci-dessus. Au cours de l'opération  
 20 37, un sceau secret est généré et transmis, par l'intermédiaire du deuxième réseau 140, au récepteur 150. L'adresse du récepteur 150 sur le deuxième réseau est déterminée en mettant en correspondance l'identifiant de l'utilisateur transmis au cours de l'opération 31 avec ladite adresse, dans une table de correspondance. Préférentiellement, le sceau secret dépend des données à transmettre, de leur nombre, de leur contenu, de la date et de l'heure  
 25 de la génération du sceau secret, de la clé privée de l'émetteur des données déterminée en correspondance avec l'identifiant de l'utilisateur transmis au cours de l'opération 1, de l'adresse internet ("adresse IP") du poste utilisateur 100 et/ou d'un numéro de la session Internet au cours de laquelle les données sont transmises. Selon un exemple de mise en oeuvre de l'opération 7, le sceau secret est obtenu par calcul d'un condensâ des données à  
 30 transmettre, par exemple sous la forme d'une séquence de 20 symboles, de chiffrement de ce condensâ par la clé privée de l'utilisateur du poste utilisateur 100 et d'extraction d'une partie du résultat de ce chiffrement.

Le lecteur pourra se référer à la figure 4 et/ou à la demande de brevet PCT/FR98/02348 pour mieux connaître des exemples d'étapes mises en oeuvre au cours

des opérations 37 et 38. Au cours de l'opération 38, l'utilisateur commun du poste utilisateur 100 et du récepteur 150 saisie le sceau secret et ce sceau secret est transmis au serveur de sécurité 170 où le sceau est vérifié, opération 39.

5 En variante, les opérations 37 à 39 sont remplacées par une opération de signature basée sur l'utilisation d'une carte à mémoire ("carte à puce") ou d'une mesure de biométrie.

A la fin de l'opération 38, les ensembles de données transmis sont donc certifiées intègres et signées par l'utilisateur qui les transmet. L'opération 39 consiste à substituer une signature dite PKI (pour Public Key Infrastructure, soit infrastructure de  
10 clés publiques) à la signature effectuée au cours des opérations 37 et 38.

Au cours de l'opération 39, les ensembles de données transmis sont signés avec la clé privée de l'utilisateur qui les a transmise (dit "signataire" des données).

Enfin, au cours de l'opération 41, les ensembles de données transmises, certifiées et signées par clé privée sont transmises à la mémoire de stockage 130 avec une  
15 date de telle manière qu'elles sont horodatées, archivées et notarisées.

Dans une application de la présente invention à une remise en main propre des ensembles de données transmises, pour chaque ensemble de données à transmettre, un destinataire est, à la suite de l'opération 41, averti de la mise à sa disposition de l'ensemble de données à transmettre et des opérations similaires aux opérations exposées  
20 ci-dessus sont mises en oeuvre pour effectuer une copie certifiée conforme sur le poste utilisateur du destinataire après avoir recueilli de sa part une signature. Un exemple d'une succession d'opérations mises en oeuvre pour cette remise en main propre est donné en figure 2.

La figure 4 représente un organigramme de mise en oeuvre d'un autre  
25 mode de réalisation de la présente invention. Dans la colonne la plus à gauche de la figure 4 sont représentées des opérations concernant un système informatique dit "émetteur" 401 mettant en oeuvre un premier support de communication. Dans la colonne à droite de la colonne la plus à gauche sont représentées des opérations concernant un premier dispositif de communication 402 mettant en oeuvre un deuxième support de  
30 communication. Dans la colonne centrale sont représentées des opérations concernant un système informatique 403 dit "récepteur" mettant en oeuvre le premier, le deuxième, un troisième et un quatrième support de communication. Dans la colonne la plus à droite sont représentées des opérations concernant un système informatique 405 dit "destinataire" mettant en oeuvre le troisième support de communication. Enfin, dans la

colonne entre la colonne centrale et la colonne la plus à droite, sont représentées des opérations concernant un deuxième dispositif de communication 404 mettant en oeuvre le quatrième support de communication.

Le système informatique émetteur 401 et le premier dispositif de communication 402 sont utilisés par un utilisateur qui souhaite transmettre des données à un utilisateur destinataire qui utilise le deuxième dispositif de communication 404 et le système informatique destinataire 405. Par exemple, le système informatique émetteur 401 est un ordinateur personnel, ou un ordinateur de réseau, connecté au réseau Internet. Par exemple, le système informatique destinataire 405 est un autre ordinateur personnel, ou un autre ordinateur de réseau, connecté au réseau Internet. Les premier et troisième réseau peuvent être confondus ou différents. Le premier et le troisième réseaux peuvent ainsi être l'Internet.

Les deuxième et quatrième réseaux peuvent, en particulier être des réseaux non filaires. Par exemple, le premier dispositif de communication 402 est un téléphone mobile ou un pageur. Par exemple, le deuxième dispositif de communication 404 est un téléphone mobile ou un pageur. Les deuxième et quatrième réseaux peuvent être confondus ou différents. En revanche, le premier et le deuxième support de communication sont différents. De plus, le troisième et le quatrième support de communication sont différents. Préférentiellement, les dispositifs de communication 401 et 404 possèdent des adresses uniques sur le deuxième et le quatrième réseau de communication, respectivement.

Selon un exemple de réalisation, le système informatique récepteur 403 est un serveur de réseau connecté à des interfaces de réseau pour communiquer sur les premier à quatrième réseaux. Dans la suite de la description de la figure 4, on considère que le système informatique récepteur 403 conserve des moyens nécessaires pour obtenir :

- une clé privée et une clé publique d'un utilisateur du système informatique émetteur 401,
- l'adresse du premier dispositif de communication 402 sur le deuxième support de communication, et
- l'adresse du deuxième dispositif de communication 404 sur le quatrième support de communication.

Par exemple, le système informatique récepteur 403 conserve en mémoire :

- la clé privée et la clé publique de chaque utilisateur susceptible de mettre en oeuvre le procédé décrit en figure 4,
- une table de correspondance entre des identifiants d'utilisateurs et des adresses sur le deuxième support de communication, et
- 5       - un moyen d'interroger une base de données conservant une table de correspondance entre des identifiants d'utilisateurs destinataires et des adresses sur le quatrième support de communication.

Selon une variante, l'adresse de l'utilisateur destinataire sur le quatrième réseau est obtenue de la part de l'utilisateur émetteur, comme dans le cas illustré en figure

10    4.

Les opérations de démarrage et d'initialisation et les opérations d'arrêt des systèmes informatiques et des dispositifs de communication ne sont pas représentées en figure 4.

15       Au cours d'une opération 408, le système informatique émetteur 401 se connecte au système informatique récepteur 403, par l'intermédiaire du premier support de communication. Au cours d'une opération 409, le système informatique récepteur 403 transmet au système informatique émetteur 401 un programme permettant de déterminer un condensé de données à transmettre.

20       Au cours d'opérations de transmission 410 et 411, le système informatique émetteur 401 transmet au système informatique récepteur 403, sur le premier support de communication :

- des données à transmettre au système informatique destinataire 405,
- un condensé des données à transmettre déterminé avec le programme transmis au cours de l'opération 409,
- 25       - un identifiant d'un utilisateur du système informatique émetteur 401 ou un identifiant du système informatique émetteur 401, et
- un identifiant du système informatique destinataire 405 et une adresse du deuxième moyen de communication 404.

30       Au cours d'une opération de mise en correspondance 412, le système informatique récepteur 403 met en correspondance ledit identifiant avec une clé privée de l'utilisateur du système informatique émetteur 401.

Au cours d'une opération de génération 413, le système informatique récepteur 403 génère une trace des données à transmettre. La trace est représentative des données à transmettre. Préférentiellement, ladite trace est représentative d'un condensé

desdites données à transmettre et de la clé privée conservée par le système informatique récepteur 403. Par exemple, ladite trace est obtenue par une opération de signature du condensât par la clé privée de l'utilisateur du système informatique émetteur 401. Ainsi, ladite trace est liée aux dites données et toute modification ultérieure des dites données est  
 5 détectable. De plus, la source des dites données est ainsi authentifiée par la clé privée de l'utilisateur.

Au cours d'une opération de mise en correspondance 414, l'identifiant de l'utilisateur du système informatique émetteur 401 est mis en correspondance avec une adresse du dispositif de communication 402 sur le deuxième support de communication.

10 Au cours d'une opération de transmission 415 d'une partie de ladite trace, au moins une partie de la trace déterminée au cours de l'opération 413 est transmise par le système informatique récepteur 403 au premier dispositif de communication 402. Par exemple, l'opération de transmission 415 comporte au cours de l'opération de troncature 416 au cours de laquelle la trace déterminée au cours de l'opération 413 est tronquée et le  
 15 résultat de ladite troncature est transmis au premier dispositif de communication 402.

Au cours d'une opération de réception 417, ladite partie de trace est reçue par le système informatique émetteur 401. Par exemple, le premier dispositif de communication 402 affiche ladite trace sur un écran de visualisation et l'utilisateur du premier dispositif de communication 402 tape ladite trace sur un clavier du système  
 20 informatique émetteur 401. Selon des variantes, l'utilisateur émetteur dicte ladite partie de trace qui est reconnue par un système de reconnaissance de voix ou l'utilisateur émetteur fournit ladite partie de trace au système informatique émetteur 401 par le biais d'une interface utilisateur quelconque.

Au cours d'une opération de transmission de ladite partie trace 418, ladite  
 25 partie de trace est transmise depuis le système informatique émetteur 401 au système informatique récepteur 403.

Au cours d'une opération de vérification 419, le système informatique récepteur vérifie la correspondance de la partie de trace reçue par le système informatique récepteur 403 avec la trace générée par le système informatique récepteur 403. La  
 30 correspondance est, dans l'exemple de la figure 4, une égalité entre la trace émise et la trace reçue. S'il n'y a pas correspondance, le système informatique récepteur indique à l'utilisateur émetteur qu'il n'a pas été authentifié, par le biais du premier support de communication ou par le biais du deuxième support de communication et invite l'utilisateur émetteur à recommencer les opérations illustrées en figure 4.

S'il y a correspondance, au cours d'une opération de mise en correspondance 420, le système informatique récepteur 403 met en correspondance lesdites données avec une clé publique de l'utilisateur émetteur.

5 Au cours d'une opération de communication 421, le système informatique récepteur 403 transmet un message, par exemple un courrier électronique, à l'utilisateur destinataire l'invitant à se connecter par le biais du troisième support de communication au système informatique récepteur 403.

10 Au cours d'une opération de connexion 422, l'utilisateur destinataire effectue la connexion entre le système informatique destinataire 405 et le système informatique récepteur 403.

Au cours d'une opération de génération d'une information confidentielle 423, le système informatique récepteur 403 génère une information confidentielle. Au cours d'une opération de transmission 424, le dispositif récepteur 403 transmet ladite information confidentielle au deuxième dispositif de communication 404, par le biais du  
15 deuxième support de communication.

Au cours d'une opération de réception 425, ladite information confidentielle est reçue par le système informatique destinataire 405. Par exemple, le deuxième dispositif de communication 404 affiche ladite information confidentielle sur un écran de visualisation et l'utilisateur du deuxième dispositif de communication 404  
20 tape ladite information confidentielle sur un clavier du système informatique destinataire 405. Selon des variantes, l'utilisateur destinataire dicte ladite information confidentielle qui est reconnue par un système de reconnaissance de voix ou l'utilisateur destinataire fournit ladite information confidentielle au système informatique destinataire 405 par le biais d'une interface utilisateur quelconque.

25 Au cours d'une opération de transmission de ladite information confidentielle 426, ladite information confidentielle est transmise depuis le système informatique destinataire 405 au système informatique récepteur 403.

Au cours d'une opération de vérification de correspondance 427, le système informatique récepteur 403 vérifie la correspondance entre l'information  
30 confidentielle transmise par le système informatique récepteur 403 et l'information confidentielle reçue par le système informatique récepteur 403. S'il n'y a pas correspondance, le dispositif informatique récepteur 403 indique à l'utilisateur destinataire qu'il n'a pas été authentifié, par le biais du troisième ou du quatrième support de communication et l'invite à recommencer les opérations 422 et suivantes.

Lorsqu'il y a correspondance, au cours d'une opération de transmission des données au système informatique destinataire 428, le système informatique récepteur 403 transmet au système informatique destinataire 405 les données à transmettre.

Préférentiellement, le système informatique 403 transmet conjointement aux données à  
5 transmettre :

- une clé publique de l'utilisateur émetteur au système informatique destinataire 405,
- la trace desdites données à transmettre calculée au cours de l'opération , et
- un programme permettant de déterminer ledit condensâ desdites données.

10 Au cours d'une opération 429, le système informatique destinataire détermine le condensâ desdites données à transmettre calculé au cours de l'opération 413 et utilise la clé publique reçue au cours de l'opération 428 pour déterminer le condensâ desdites données qui a servi à générer la trace transmise au cours de l'opération 428. Lorsque les deux condensâ sont égaux, l'utilisateur destinataire a l'assurance que c'est  
15 l'utilisateur émetteur qui a transmis les données à transmettre et que ces données n'ont pas été modifiées depuis qu'elles ont été transmises par l'utilisateur émetteur.

Selon des variantes, les opérations présentées en figures 1, 2 ou 3 et les opérations présentées en figure 4 sont combinées de telle manière que, dans ces variantes, une clé jetable est utilisée pour la transmission des données d'un système informatique à  
20 un autre et une trace qui dépend des données à transmettre et, éventuellement d'une clé privée de l'utilisateur émetteur, est mise en oeuvre.



## REVENDICATIONS

1. Procédé de certification, caractérisé en ce qu'il comporte :

- 5           - une opération de transmission (4, 5) de données depuis un système informatique émetteur (100) à un système informatique récepteur (130), sur un premier support de communication,
- une opération de génération (7) d'une trace desdites données représentatives desdites données, par le système informatique récepteur,
- 10          - une opération de transmission (7) d'une partie de ladite trace à un dispositif de communication, sur un deuxième support de communication différent du premier support de communication,
- une opération de réception (8) de ladite partie de trace par le système informatique émetteur,
- une opération de transmission (8) de ladite partie trace depuis le système
- 15          informatique émetteur au système informatique récepteur, et
- une opération de vérification (9) de la correspondance de la partie de trace reçue par le système informatique récepteur avec la trace générée par le système informatique récepteur.

2. Procédé selon la revendication 1, caractérisé en ce que, au cours de ladite  
20 opération de génération de ladite trace, ladite trace est représentative d'un condensé desdites données.

3. Procédé selon l'une quelconque des revendications 1 ou 2, caractérisé en ce qu'il comporte une opération de transmission (1) d'un identifiant d'un utilisateur du système informatique émetteur.

25          4. Procédé selon la revendication 3, caractérisé en ce qu'il comporte une opération de mise en correspondance (7) dudit identifiant avec une adresse du dispositif de communication sur le deuxième support de communication.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que, au cours de ladite opération de génération de ladite trace, ladite trace est représentative d'une  
30 clé privée conservée par le système informatique récepteur.

6. Procédé selon l'une quelconque des revendications 3 ou 4 et selon la revendication 5, caractérisé en ce qu'il comporte une opération de mise en correspondance (7) dudit identifiant avec ladite clé privée.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il comporte une opération de troncature (7) de ladite trace, et en ce que au cours de l'opération de transmission d'une partie de ladite trace, le résultat de ladite troncature est transmis.

5 8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que le premier support de communication est l'Internet.

9. Procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce que le deuxième support de communication est un réseau sans fil.

10 10. Procédé selon l'une quelconque des revendications 1 à 9, caractérisé en ce que, au cours de l'opération de transmission desdites données (5), un identifiant d'un système informatique destinataire est transmis, ledit procédé comportant une opération de transmission desdites données depuis le système informatique récepteur à un système informatique destinataire.

15 11. Procédé selon la revendication 10, caractérisé en ce qu'il comporte une opération de mise en correspondance desdites données avec une clé publique et en ce que au cours de l'opération de transmission desdites données audit système informatique destinataire, ladite clé publique est transmise.

20 12. Procédé selon l'une quelconque des revendications 10 ou 11, caractérisé en ce qu'il comporte une opération de génération d'une information confidentielle par le système informatique récepteur et une opération de transmission à un deuxième dispositif de communication d'une information confidentielle à une dispositif de communication sur le deuxième support de communication, par le système informatique récepteur, une opération de réception de ladite information confidentielle par le système informatique récepteur, sur le premier moyen de communication et une opération de vérification de  
25 correspondance entre l'information confidentielle transmise par le système informatique récepteur avec l'information confidentielle reçue par le système informatique récepteur.

13. Dispositif de certification, caractérisé en ce qu'il comporte :

- un moyen de transmission de données depuis un système informatique émetteur à un système informatique récepteur, sur un premier support de communication,
- 30 - un moyen de génération d'un trace desdites données représentatives desdites données, par le système informatique récepteur,
- un moyen de transmission d'au moins une partie de ladite trace à un dispositif de communication, sur un deuxième support de communication différent du premier support de communication,

- un moyen de réception de ladite trace par le système informatique émetteur,
  - un moyen de transmission de ladite trace depuis le système informatique émetteur au système informatique récepteur, et
  - un moyen de vérification de la correspondance de la trace reçue par le système
- 5 informatique récepteur et de la trace générée par le système informatique récepteur.

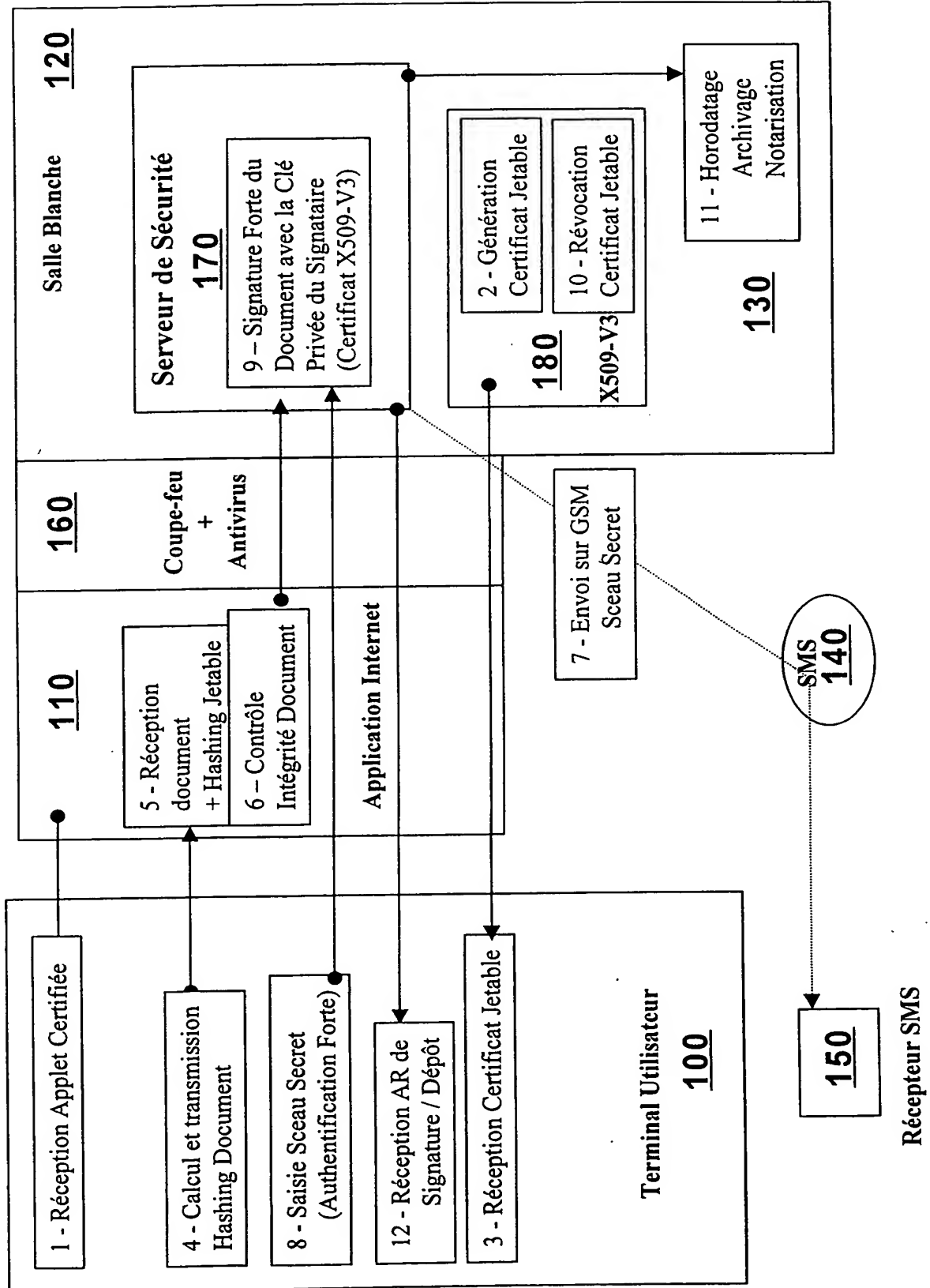


Fig. 1

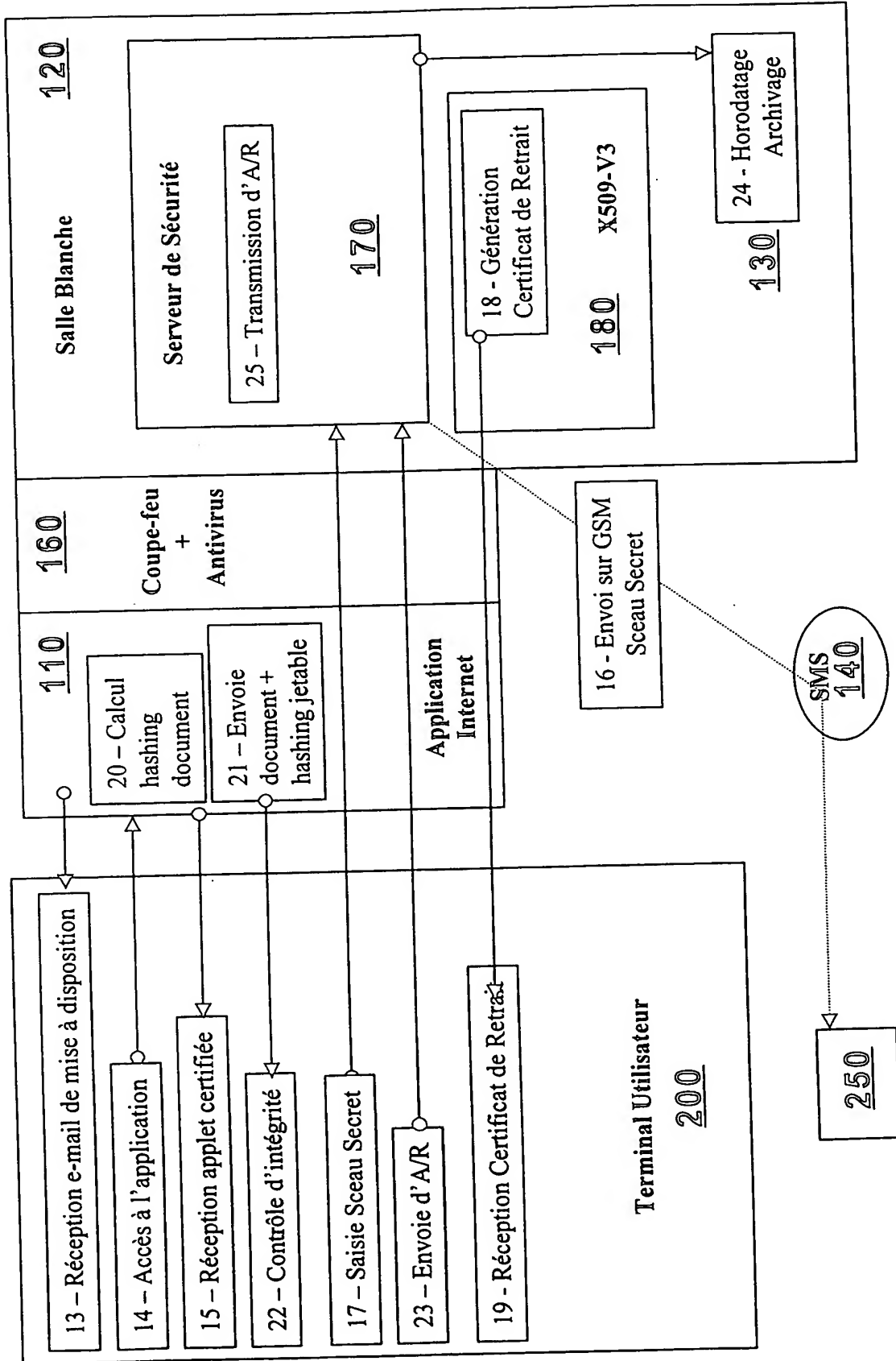


Fig. 2

Récepteur SMS

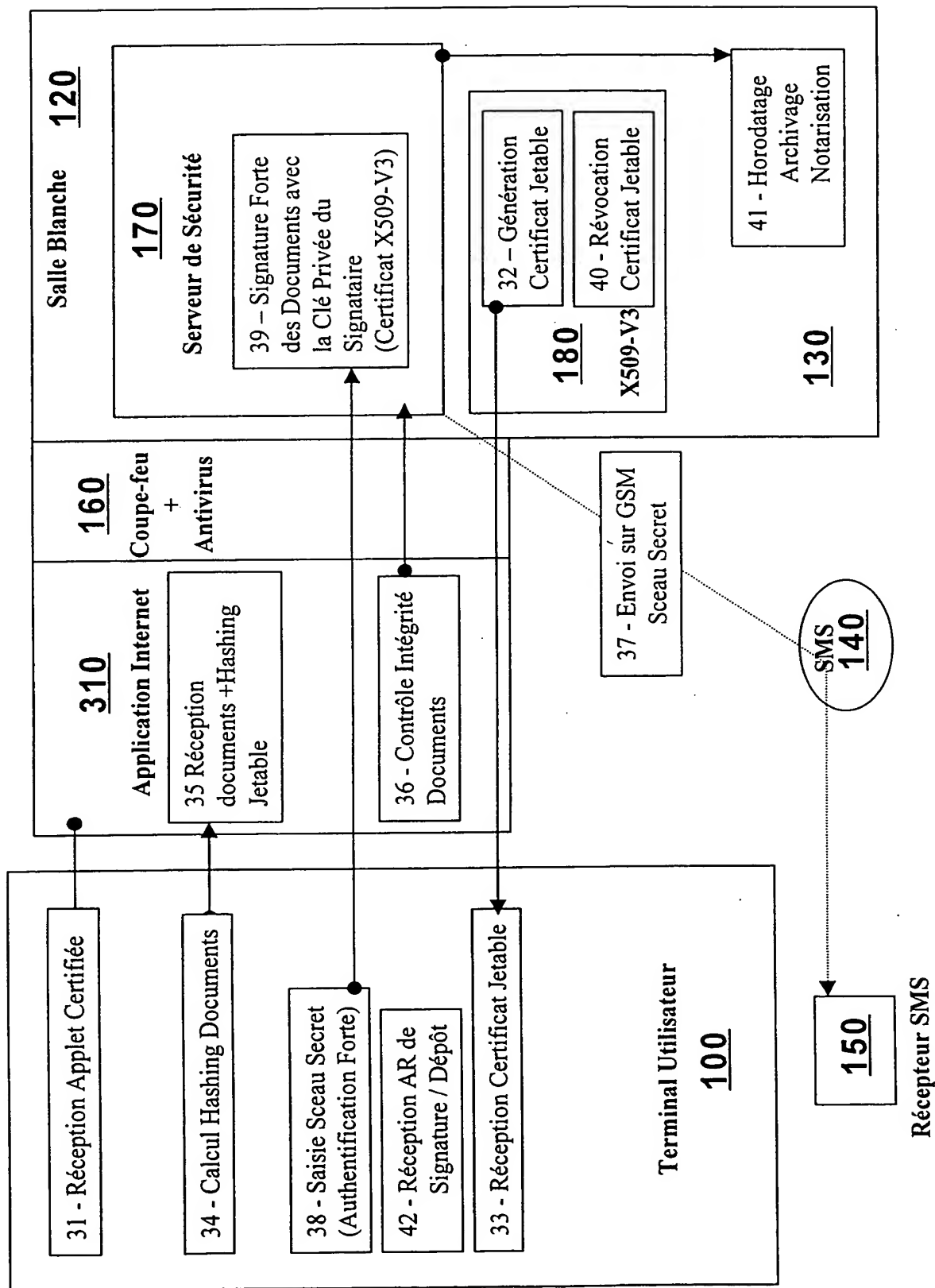


Fig. 3

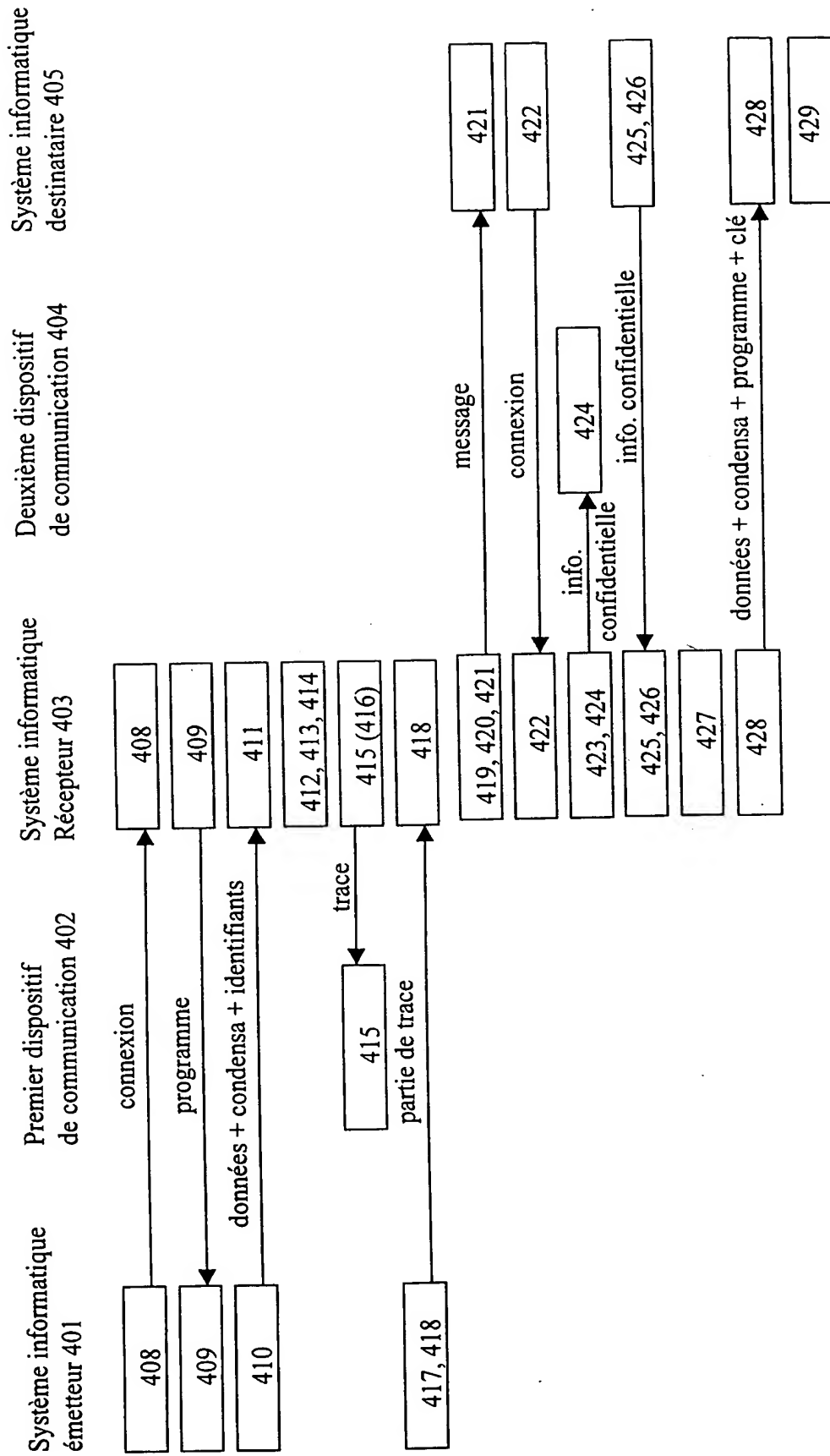


Fig. 4

**THIS PAGE BLANK (USPTO)**